BASLE II and Management of Operational Risks
Myth and Reality

FLUX Risk Services is a consultancy firm that works extensively for the insurance industry as risk surveyors and loss adjusters in the banking sector. Over the last 15 years, our involvement in speciality risks insurance (Bankers Blanket Bond, Computer Crime, Professional Indemnity and Directors & Officers policies) has given us a unique insight into both risk mitigation and insured losses in a variety of financial institutions worldwide.

Introduction

Now that Y2K and the introduction of the EURO are well behind us, banks are slowly starting to turn to the practical implications of the Basle II operational risk directive, which has recently been clarified (again) and is now expected to come into force at the end of 2006.

The Operational Risk Directive (ORD) puts forward two key concepts:

- Three measurement methodologies for calculating operational risk capital charges (a fourth may become available in future).
- The implementation of a framework for effective management and supervision of operational risk (defined as "identification, assessment, monitoring and control/mitigation of risk").

Based on our experience of work practices and operational controls in banks, this document attempts to set out our thoughts on operational risk management in the light of proposals made by the Risk Management Group of the Basel Committee.

The Measurement Methodologies

The three methods (Basic Indicator, Standardised and Internal Measurement) have differing levels of sophistication but are based on the same fundamental principles. In short, a capital factor is applied either to a bank's gross income (Basic Indicator) or to financial indicators such as gross income or average assets/throughput, broken down by business unit and business line (Standardised and Internal Measurement). The capital factor will be essentially set by regulators (Basic Indicator, Standardised) and/or the banks themselves (Internal Measurement) based on either generally available historical industry-wide operational loss data or in combination with the specific bank's own internal loss data.

Drawing on our own experience the foregoing has certain drawbacks:

- Initial projections conducted in certain banks (and by ourselves) using the three different methodologies have given significantly differing capital charges – this often by a factor in excess of five! As the less onerous method would only seem to be available to larger banks that may have a broad spectrum of internal loss data stretching back some years, others may be penalised unduly. In this context we note that the issue of setting a "floor" or lower minimum limit for the Internal Measurement method is still under discussion.
- Our own loss data of insurance claims show that operational loss types vary significantly from country to country. This, all the more, as banks are tending to centralise certain business lines in certain countries. It is clear that in certain locations significant losses are essentially concentrated in one or two businesses (e.g. private banking, asset management or investment banking). This would pre-suppose differing capital charges being set in different countries to be at all realistic. Also banks specialising in "high risk" businesses will presumably be subject to higher capital charges.
  For the record, our historical insurance data over the last 5 years would suggest that operational losses broadly conform to the following breakdown:

By Business by amount	
Commercial Banking	10%
Retail (including private banking)	65%
Trading and Sales	20%
Other	5%

By Type by amount	
Processing errors	50%
Legal/Compliance issues	20%
Internal fraud	15%
External fraud	5%
Miscellaneous other (including system failures)	10%

- Those banks that have put in place the necessary structure to collect internal operational loss data, have to an extent realised that it is not indicative and often misleading in respect of future loss scenarios. For example, a large loss in one area draws in resources and may divert attention from potential risks in another. Further, our own experience would suggest that for small and even medium banks, loss history over an extended period is patchy at best and will

probably never be representative. Again, this may mean that such banks would be excluded from using the more sophisticated Internal Measurement approach.

To close, we would just highlight that those rare banks that have put in place a process to identify and centralise operational loss data have found this to be more difficult than initially envisaged. This especially, when having to cover a wide range of subsidiaries over an extended geographic area which requires an effective decentralised data gathering organisation. Quite apart from problems caused by differing systems or accounting standards (much of the loss information can be taken from account data), definition of loss events can create difficulties when these arise from more than one initial cause. Also, the time lag that often occurs between a loss event and calculation of the final loss amount can make the initial information obsolete or erroneous (e.g. the control problem has long since been resolved, no financial loss was sustained *in fine,* or insurance covered part of the loss).

Sound Operational Practices

In their document on "*Sound practices for the management and supervision of operational risk*", the Basle Committee set out 10 general principles for developing an appropriate risk management environment. It is not the intent here to review all of these, as many are self-evident and have been in existence within the industry for some time. Nonetheless, we would highlight some key points below that may be of interest.

- **Responsibility of the Board for identification, assessment, monitoring and control/mitigation of operational risk.** With few exceptions, the boards of banks do not include members who have significant operations experience. More often than not they are drawn from other areas such as the front office or credit. Consequently, it is not always easy for board members to weigh up operational risk control issues that often impact revenue generation. In this context, we note that such issues are too often presented to them in a vague or incomprehensible manner after having been "screened" by internal corporate politics. It is therefore essential that there is general agreement across the Bank on a system to quantify risk issues. The implementation of a simple scoring system (good/bad, red/green) based on pre-defined criteria should enable the board to assess and monitor operational risk rapidly. Such systems have been developed for credit risk in the past and can now be adapted for operational risk.
- **Documentation of Policies.** In our experience, whilst procedures are extensively documented there are relatively few banks with comprehensive policies or standards. Policies are the cornerstone of the entire process to the extent that they set out the standards that the organisation wants to follow and therefore in a sense defines its appetite for risk. Without policies and

standards it is impossible to assess risk, as there is nothing to measure against. Thus although the Basle Committee only addresses policies under principle 6, we would suggest that before attempting to implement any risk management process a comprehensive set of policies needs to be developed. These should cover the entire spectrum of operations, including IT, new product introduction, information security, outsourcing and continuity of business.

- **Organisation.** Although only addressed indirectly by the Basle Committee, the creation of an effective operational risk structure is critical. Within banks today we find a plethora of units with responsibility for aspects of operational risk (audit, internal control, insurance managers, IT security, physical security, contingency planning etc.). Very often these units do not communicate effectively, their responsibilities overlap and they are too far down in the hierarchy of the organisation. A single risk structure with direct access to the board needs to be set up that ties together the different strands of risk management, especially IT and non IT related aspects. Although there is no ideal structure, we believe that there is a good argument for bringing together credit, market and operational risk. The addition of the insurance manager, IT and physical security to such a division enhances co-operation, provides a critical mass and should also provide input from a wider spectrum within the business.

  In certain banks the “tops down” versus “bottoms up” argument is still in full swing. From our perspective it is clear that whilst guidance and standards have to come down from the top, a bottoms up approach is essential. Both management buy-in across the organisation and reliable decentralised data input at the lowest level are critical. The creation of a network of risk management correspondents throughout the business is the obvious solution.

- **Identifying and Assessing Risk.** Under Principle 4, the Basle Committee highlights methods for identifying and assessing operational risk on an ongoing basis. These include self-assessment, risk mapping, key risk indicators or scorecards. Whilst all have their merits and some may be better suited to certain businesses, they all take time to implement and have a price tag that can be substantial. For example, in today’s business environment the pace of change is such that risk mapping can become rapidly obsolete and therefore requires constant adjustment as processes are modified.

  Our own preference is for a mixture of the above within a process that is simple and flexible. Experience has taught us that any given process can be secured to a high degree (99%) by no more than 10 or so controls. We have evolved a method whereby all units within an organisation establish such controls or “key risk indicators” and these are monitored against agreed standards that they themselves define to obtain management buy-in. Such

data is then aggregated to provide an overview of risk points within the organisation via a scorecard. This process can then be enhanced by formal self-assessments, which have a wider scope and are conducted on a more extended cycle and/or the results of internal audits.
Of note, is the fact that certain banks are now also tying in such a system to quality or performance management initiatives (e.g. Balanced Score Card). Consequently they prefer to talk of "quality" rather than "key risk" indicators.

- **Monitoring and Controlling Risk.**
  Drawing on the experience of those that have already started to implement Basle II, the nub of the problem is bringing together the different strands (historic loss data, key risk indicators, self-assessment) and create a risk management process that can pinpoint and keep track of potential or actual control issues rapidly. Not only does this process have to be able to adapt to changes in the business environment, but also in the final analysis it must be able to synthesise the results for senior management and the board. Whilst automation is the key, the underlying basic concepts should be kept simple. In our experience, the scope of operational risk (in a sense it covers everything that is not credit or market risk) means that complex models tend to fail or produce results that are too outdated to be relevant. The system has to be forward looking, identify the problems and resolve them before they generate losses.
  Consequently, certain banks have found it easier and cheaper to use split systems or databases. One is designed to drive the operational risk capital calculation, the other is used for identifying, monitoring and reporting operational risk issues.

- **Risk Mitigation.** Although perhaps somewhat sceptical initially, the Basle Committee does now see insurance as a risk mitigation tool for "low frequency, high severity losses". In fact the vast majority of banks today are insured against internal or external fraud, computer crime or professional negligence risks. Further, contrary to what the Committee may believe, most if not all reputable insurers do pay out promptly provided claims are within policy terms. If they didn't, banks would presumably have stopped buying insurance long ago. In today's market, putting together an effective and adapted operational risk insurance programme for a bank is a specialised and increasingly costly business. Consequently, it is important that the insurance manager (often referred to as the "risk manager") is an integral part of the risk management structure. For the bank to get value for money he has to understand the business, associated risks and the system that is in place to manage these. If nothing else, he will have to explain these to actual or potential insurers.

Lastly it should be remembered that insurance policies are traditionally written on a legal vehicle basis, not by business line. To obtain the maximum advantage from risk management systems it may be necessary to cut data not just by business line but also by legal entity.

Conclusion

Of the 45 or so banks that we have reviewed in the last 2 years, only a handful are anywhere near attaining the standards put forward on operational risk management in Basle II. Further, our experience of insurance claims show time and time again that substantial operational losses in banks, be they due to fraud or errors, are caused by a breakdown or absence of basic controls. Very often, more than one within a specific process. The issue is therefore rarely one of complexity. Further, in a large number of cases there are various warning signals that should have alerted management to a problem but were incorrectly assessed or ignored.

Consequently, we can only suggest that banks that are developing operational risk management processes concentrate on the basics. The implementation of simple tools effectively across an organisation will go a long way to reducing losses substantially. When all is said and done the objective is to improve controls and reduce risks going forward, not just create another reporting system that shows what has happened in the past.

The old KISS adage "Keep it Stupid, Keep it Simple" still applies.

PATRICK MAUGHAN

January 2003

email : maughan.patrick@fluxrisk.com
tel : 0032.2.725.11.79 - fax : 0032.2.725.17.47

FLUX RISK SERVICES SA
16 Av de la Sablière
1160 BRUSSELS - BELGIUM
http://www.fluxrisk.com

FLUX Ops Risk Management Process